

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-141192

(43)Date of publication of application : 20.05.1994

(51)Int.Cl.

H04N 1/44  
G09C 5/00

(21)Application number : 04-327141

(71)Applicant : PANPUKIN HOUSE:KK

(22)Date of filing : 26.10.1992

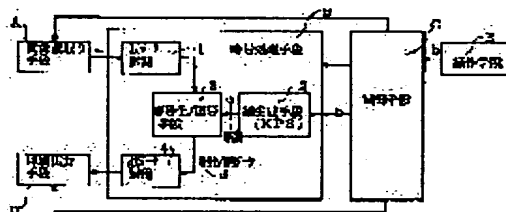
(72)Inventor : IMAI HIDEKI

## (54) COPYING MACHINE WITH CIPHER FUNCTION

## (57)Abstract:

PURPOSE: To provide the copying machine with cipher function prepares enciphered documents and drawings, which can be deciphered by only a specific person, without preliminary arrangement and cipher key delivery.

CONSTITUTION: This cipher key generating system consists of a picture read means A which reads information of documents, drawings, or the like, an enciphering/deciphering means 3 which enciphers or decipheres information, a key generating means 2 which prepares a cipher key used for enciphering/deciphering, a control means C for various control, a print output means D which prints out picture information, and an operation means E for operation. This system uses a key sharing type cipher (KPS) theory, and the identifier of a specific entry or names specifying a name specifying a document, a drawing or the like is inputted to prepares a cipher key.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平6-141192

(43)公開日 平成6年(1994)5月20日

(51)Int.Cl.<sup>5</sup>

H 0 4 N 1/44

G 0 9 C 5/00

識別記号

庁内整理番号

2109-5C

8837-5L

F I

技術表示箇所

審査請求 未請求 請求項の数3(全 5 頁)

(21)出願番号

特願平4-327141

(22)出願日

平成4年(1992)10月26日

(71)出願人 393009356

株式会社バンプキンハウス

神奈川県厚木市飯山1620番地の1 アメニ

ティヒル本厚木717

(72)発明者 今井 秀樹

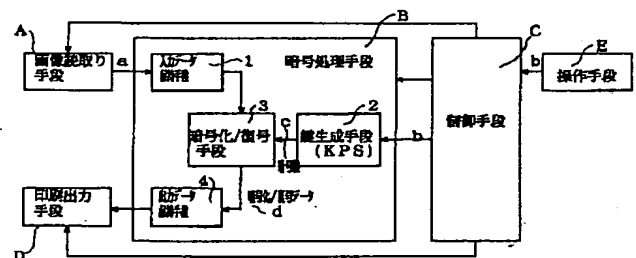
神奈川県横浜市南区六ツ川3-76-3

(54)【発明の名称】 暗号機能付き複写機

(57)【要約】 (修正有)

【目的】 前もって打ち合せや暗号鍵の配送を行わずに特定の人だけが復号できる暗号化書類、図面を作成する暗号機能付き複写機を提供する。

【構成】 書類、図面等の情報を読取る画像読取り手段、情報の暗号化又は復号を行う暗号化／復号手段、暗号化／復号に用いられる暗号鍵を生成する鍵生成手段、各種の制御を行う制御手段、画像情報を印刷出力する印刷出力手段、そして操作を行う為の操作手段より成る。この暗号鍵生成システムは鍵共有方式暗号システム(KPS)理論を用い、特定のエンティティの識別子、又は書類、図面等を特定する名前を入力して暗号鍵を生成することを特徴とする。



(2)

1

## 【特許請求の範囲】

【請求項1】 紙などの媒体に描写された画像情報及び／またはそれを符号化した情報を入力し、これを暗号化した状態で印刷し、又印刷された暗号画像を読みとって復号し元の画像に戻して印刷及び／またはディスプレイに表示を行う暗号機能付き複写機において、各エンティティ（人、装置等）が、半固定的に用いるもので任意に定められる公開の識別子を有し、センタ（管理者）だけが持つ特別なアルゴリズム（データ）と、エンティティの識別子に一方方向性でランダムな単射を行う識別子変換を施したものとを演算させて、エンティティに固有な秘密アルゴリズム（データ）を生成してエンティティがこれを保持し、暗号化／復号を行う際に任意エンティティの識別子または任意の名前等を識別子として識別子変換を施したものと自分の秘密アルゴリズムとを演算させることにより、打合せや第三者による配送を必要とせず、自分と任意のエンティティ又は任意の名前等に固有の鍵（暗号鍵）を生成し、この鍵を用いて、前記画像情報の暗号化／復号を行うことを特徴とする暗号機能付き複写機。

【請求項2】 前記秘密アルゴリズムに識別子を入力して暗号鍵を生成する鍵生成手段と暗号化／復号手段を内蔵した外部装置を接続し、外部装置内で暗号鍵の生成及び画像情報の暗号化または暗号画像の復号を行うことを特徴とする請求項1の暗号機能付き複写機。

【請求項3】 前記秘密アルゴリズムに識別子を入力して暗号鍵を生成する鍵生成手段を内蔵した外部装置を接続し、外部装置内で生成させた暗号鍵を用いて暗号化／復号を行う暗号化／復号手段を内蔵することを特徴とする請求項1の暗号機能付き複写機。

## 【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、暗号機能付き複写機に関する。

【0002】

【従来技術】 書類、図面などの情報を複写機で複写を行うようにして入力し、暗号化した状態で印刷して保管することによって内容の漏洩を防ぎ、必要なときに復号して元に戻すことを可能とした装置が提案された。

【0003】

【発明が解決しようとする問題点】 特定の人だけが復号できる暗号化書類、図面を作成する場合、暗号鍵の打合せが必要であり、さらにその鍵を安全に保管する為の管理が必要となる。又、多くの異なる書類、図面を暗号化する時に、同一の暗号鍵を用いたのでは安全性に問題があり、異なる暗号鍵を用いるにはその決定と管理が大変である。さらに、印刷された暗号書類、図面を、暗号化したのとは別の場所にある装置で復号する場合、暗号鍵の打ち合せや配送が必要である。

【0004】

2

【課題を解決する為の手段】 本発明は、任意のエンティティの識別子を入力するだけで暗号鍵を生成する鍵共有方式暗号システム（以下、KPSという）の理論を用い、特定のエンティティの識別子、又は書類、図面等を特定する名前を入力して暗号鍵を生成し、暗号化を行うことにより、暗号鍵の打ち合せと保管の管理が不要で、且つ特定のエンティティだけが復号を行うことができると共に書類図面の名前を入力するだけで暗号処理を行うことが可能な暗号機能付き複写機を実現した。

【0005】

【実施例】 図1は、本発明による暗号機能付き複写機の一実施例を示した図である。本暗号機能付き複写機（以下、本機と称する）は、画像読取り手段A、暗号処理手段B、制御手段C、印刷出力手段D、及びユーザが本機を制御する為の操作手段Eから構成される。暗号処理手段Bは、入力データ保持手段1、鍵生成手段2、暗号化／復号手段3、出力データ保持手段4で構成される。

【0006】 ここで、打合せや第三者による暗号鍵

（鍵）の配送を必要とせず、自分と任意のエンティティに固有の鍵を生成するKPSについて説明する。エンティティとは、一般に通信に於ける当事者となる人や装置などを示すが、ここでは人間、文書図面、装置、及びそれらを構成要素とするシステムを含む。

【0007】 エンティティ  $i$  が、半固定的に用いるもので任意に定められる公開の識別子を有し、これを識別子  $Y_i$  とし、これに一方方向性でランダムな単射を行う識別子変換  $F$  を施したものを  $Z_i$ （数式1）とする。センタだけが持つ特別なアルゴリズム（データ） $G$  と、前記  $Z_i$  とを演算させて、エンティティ  $i$  に固有な秘密アルゴリズム（データ） $X_i$ （数式2）を生成する。

【数1】

$$Z_i = F(Y_i)$$

【数2】

$$X_i = G(Z_i)$$

エンティティ  $i$  は、自分の秘密アルゴリズム  $X_i$  にエンティティ  $j$  の識別子  $Y_j$  を識別子変換したものの  $Z_j$  または任意の名前等を識別子  $Y_x$  として識別子変換したものの  $Z_x$  を入力し、演算させて（数式3、4）、エンティティ  $j$  との共通な暗号鍵  $k_{ij}$  または任意の名前に固有の暗号鍵  $k_{ix}$  を生成させることができる。またエンティティ  $j$  の秘密アルゴリズム  $X_j$  に、エンティティ  $i$  の識別子  $Y_i$  を識別子変換した  $Z_i$  を入力して演算し（数式5）、鍵  $k_{ji}$  を生成させることができ、これが前記  $k_{ij}$  に等しい（数式6）ので、エンティティ  $i$  が暗号鍵  $k_{ij}$  で暗号化した内容は、エンティティ  $j$  に復号させることができる。暗号鍵  $k_{ix}$  を用いて暗号化した内容は、秘密アルゴリズム  $X_i$  を持つエンティティ  $i$  以外では復号できない。

【数3】

$$k_{ij} = X_i(Z_j)$$

50

(3)

3

【数4】

$$k i x = X i (Z x)$$

【数5】

$$k j i = X j (Z i)$$

【数6】

$$k i j = k j i = k$$

KPSの理論的な詳細については、文献1から文献5等に記述されている。

【0008】識別子を入力して暗号鍵を生成する鍵生成手段2は、図2のように構成される。前述の識別子変換Fを含む識別子変換手段5、前記秘密アルゴリズムを格納する秘密アルゴリズム格納手段6、及びそれらから暗号鍵を生成する演算手段7で構成される。

【0009】図3は、本発明請求項2の一実施例を示す図である。図中A、C、D、E及び1から4は図1に同じである。本装置は、インタフェースPを通じて鍵生成手段2と暗号化／復号手段3を内蔵した外部装置Qと接続し、鍵生成及び暗号処理を外部装置Qで行わせる。操作手段Eから入力されたエンティティの識別子bが、制御手段CからインタフェースPを経て外部装置Q内の鍵生成手段2へ送られ、暗号鍵cが生成されて暗号化／復号手段3に送られる。画像読取り手段Aで読取られた画像情報aは入力データ保持手段1を経て制御手段Cへ送られ、インタフェースPを通じて外部装置Qの暗号化／復号手段3へ送られ、暗号鍵cを用いて暗号化／復号が実行される。暗号／復号データは制御手段Cにより、出力データ保持手段4を経て印刷出力手段Dに送られ、用紙上に印刷出力される。

【0010】図4は、本発明請求項3の一実施例を示す図である。図中A、B、C、D、E及び1から4は図1に同じである。本装置は、暗号処理手段Bを有し、インタフェースPを通じて鍵生成手段2を内蔵した外部装置Qと接続され、外部装置Qの鍵生成手段2で生成した暗号鍵cを用いて暗号処理手段Bで暗号化／復号をおこなう。操作手段Eから入力されたエンティティの識別子bが、制御手段CからインタフェースPを経て外部装置Q内の鍵生成手段2へ送られ、暗号鍵cが生成され、インタフェースPを経て制御手段Cから暗号処理手段B内の暗号化／復号手段3に送られる。画像読取り手段Aで読取られた画像情報aは入力データ保持手段1を経て暗号化／復号手段3へ送られ、ここで暗号鍵cを用いて暗号化／復号が実行され、出力データ保持手段4を経て印刷出力手段Dで用紙上に印刷出力される。

【発明の効果】本発明は、特定の相手だけが復号できる暗号化書類、図面を作成する場合に、暗号鍵の打合せや管理を不要とする。さらに、暗号化する書類、図面の名前などを識別子として入力し、それらに固有の暗号鍵を生成させて暗号化／復号を行うことにより、暗号処理を簡便にすると共に安全性を高めることができる。さらに、暗号鍵の生成、又は暗号鍵の生成と暗号処理手段を

4

外部装置で行うことにより、暗号化して印刷された書類、図面を、暗号化した装置とは別の場所にある装置で復号させることができると共に、複数のエンティティが独自に鍵生成手段または鍵生成手段と暗号化／復号手段とを内蔵した外部装置を所有することにより、一台の暗号機能付き複写機をそれぞれのエンティティが各自で鍵を管理して使用することを可能とした。

【図面の簡単な説明】

【図1】本発明請求項1の一実施例とその動作を説明する図である。

【図2】鍵生成手段の一実施例とその動作を説明する図である。

【図3】本発明請求項2の一実施例とその動作を説明する図である。

【図4】本発明請求項3の一実施例とその動作を説明する図である。

【符号の説明】

- A 画像読取り手段
- B 暗号処理手段
- C 制御手段
- D 印刷出力手段
- E 操作手段
- P インタフェース
- Q 外部装置
- a 画像情報
- b 識別子
- c 暗号鍵
- d 暗号化／復号データ
- 1 入力データ保持手段
- 2 鍵生成手段
- 3 暗号化／復号手段
- 4 出力データ保持手段
- 5 識別子変換手段
- 6 秘密アルゴリズム格納手段
- 7 演算手段

【文献1】松本勉、今井秀樹、"第3の鍵共有方式"、1986年暗号と情報セキュリティワークショップ講演論文集、1986年8月。

【文献2】松本勉、今井秀樹、"簡便な暗号鍵共有方式"、電気通信学会誌IT86-54、P-29~34、1986年9月。

【文献3】松本勉、今井秀樹、"キー プレディストリビューション システムの方式" ("KEY PRE DISTRIBUTION SYSTEM BASED ON LINEAR ALGEBRA")、第9回情報理論とその応用シンポジウム、SITA'86、1986年10月。

【文献4】松本勉、今井秀樹、"アブライジング ザ キー プレディストリビューション システム トウ エレクトロニク メール アンド シグネチャ"、情報

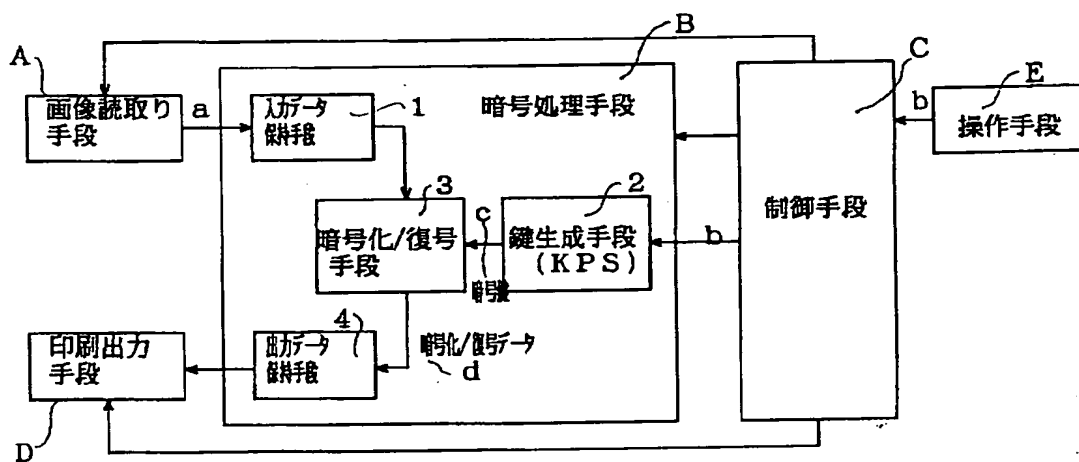
(4)

5  
理論とその応用シンポジウム、SITA' 87, 1987年11月。(Tsutomu MATSUMOTO and, Hideki IMAI, "Applying the Predistribution System to Electronic Mails and Signatures", SITA' 87, NO V., 1987.)

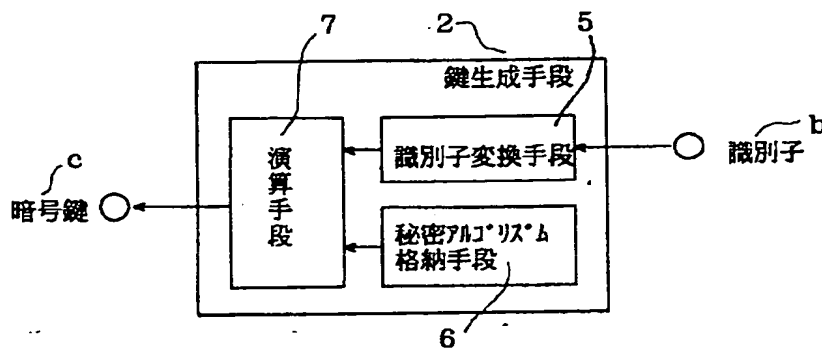
【文献5】松本勉、今井秀樹、"パフォーマンス オブ リニア スキーム フォア ザ キー プレディスト

6  
レビュー システム"、IEICE情報セキュリティ技術報告、5月20日号、1989年。(Tsutomu MATSUMOTO and, Hideki IMAI, "Performance of linear schemes for the Key Predistribution System", IEICE Technical report on Information Security, May 20, 1988.)

【図1】

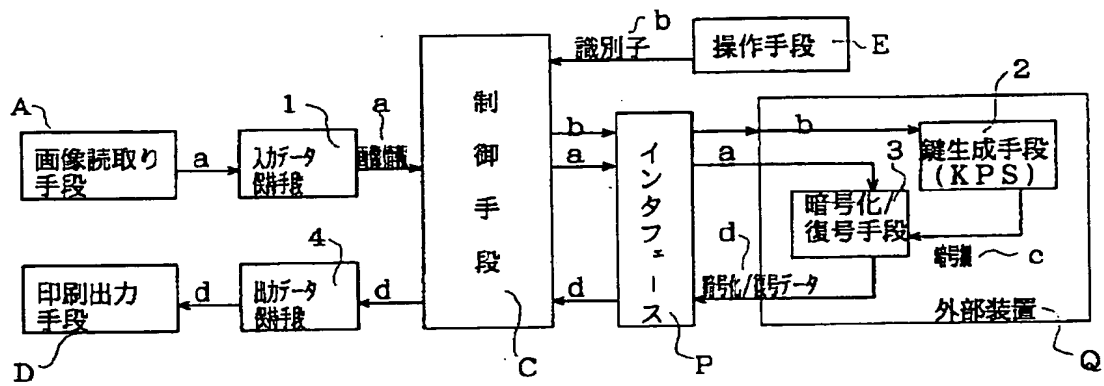


【図2】



(5)

【図3】



【図4】

